

Cybersecurity and Data Privacy Update

June 25, 2025

If you have any questions regarding the matters discussed in this memorandum, please contact the following attorneys or call your regular Skadden contact.

Nicola Kerr-Shaw

Counsel / London
44.20.7519.7101
nicola.kerr-shaw@skadden.com

Aleksander J. Aleksiev

Associate / London
44.20.7519.7000
aleksander.aleksiev@skadden.com

Alex Smallwood

Associate / London
44.20.7519.7202
alex.smallwood@skadden.com

This memorandum is provided by Skadden, Arps, Slate, Meagher & Flom LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This memorandum is considered advertising under applicable state laws.

One Manhattan West
New York, NY 10001
212.735.3000

22 Bishopsgate
London EC2N 4BQ
20.7519.7000

UK Bill Would Increase Cybersecurity Standards for Critical Infrastructure Operators

Recent months have seen a spate of high-profile cyber incidents that have affected UK companies and disrupted supply chains, keeping cybersecurity on the front pages and at the top of UK companies' agendas. In response to the growing threat of cyber incidents for UK business, the government has proposed a Cyber Security and Resilience Bill, and the Department for Science, Innovation and Technology recently released a [policy statement providing further detail](#) on the proposed measure.

The Bill would reform the UK's 2018 Network and Information Security (NIS) Regulations by introducing new obligations on critical infrastructure operators to implement security measures, notify regulators more promptly about cyber incidents and secure their supply chains. For background, see our 8 August 2024 client alert "[New UK Government Announces AI and Cybersecurity Reforms](#)" and our 15 October 2024 client alert "[Timeline Set for UK Cybersecurity and Resilience Reforms](#)."

Many elements of the Bill are analogous to the EU's NIS2 Directive (which updated the EU's version of the UK's NIS Regulations) and Digital Operational Resilience Act (DORA). See our 18 July 2024 client alert "[The EU's Digital Operational Resilience Act \(DORA\) – 2024 Update](#)" and our 11 October 2024 client alert "[Navigating the New Cybersecurity Landscape: Key Implications of the EU's NIS 2 Directive](#)."

Below we set out key features of the Bill and compare these with the EU's reforms.

Key Proposals

Service Providers and (Potentially) Data Centres Brought Into Scope

The NIS Regulations apply to a defined set of "operators of essential services" and "relevant digital service providers" in critical infrastructure sectors, including energy, transport, health, water and digital infrastructure. The Bill will expand their scope to encompass IT-managed service providers (MSPs). The government expects around 1,000 MSPs to be captured by the Bill. The government is also "considering" making data centres with 1 megawatt or greater capacity subject to the NIS Regulations.

An expansion of the NIS Regulations to cover MSPs and data centre providers would mirror the extension of the EU's NIS2 to reach MSPs and data centre providers. However, unlike NIS2, the UK government would exempt companies operating in a broader set of sectors, such as postal services, waste management, chemical, food, manufacturing and research.

UK Bill Would Increase Cybersecurity Standards for Critical Infrastructure Operators

New Oversight of ‘Critical Suppliers’

The Bill will introduce a power for the UK government to designate specific high-impact suppliers as “designated critical suppliers” (DCSs). DCSs will be subject to the obligations under the Bill similar to those of other operators of essential services.

The DCS concept does not exist in the EU’s NIS2, but is analogous to the “Critical ICT Third-Party Provider” concept under the EU’s DORA and the UK Treasury’s “Critical Third-Party” rules.

Increased Incident Reporting

The government proposes to make the NIS Regulations’ cyber incident reporting obligations stricter by:

- Expanding incident reporting criteria to require incidents that are *capable* of having a significant impact on the relevant service to be reported — not just incidents that *actually* had a significant impact.
- Lowering the timeframe for initial incident reports from 72 hours to 24 hours.
- Requiring notifications to be made both to the UK National Cybersecurity Centre and to the relevant sectoral regulator (*e.g.*, for energy companies, Ofgem).
- Requiring entities to report incidents to customers.

These changes are similar to those introduced by the EU’s NIS2.

Binding Technical Requirements

The government proposes to align the National Cybersecurity Centre’s Cyber Assessment Framework (CAF), a cybersecurity standard, with European Union Agency for Cybersecurity (ENISA) guidance issued under NIS2. The government also proposes to make the CAF binding upon regulated entities.

These changes are intended to align the cybersecurity risk-management measures required under the Bill with those required under NIS2.

New Fees for Regulated Entities

To offset the increased cost to the government of overseeing and enforcing the Bill, the government will impose new fees on entities regulated under the Bill. This is analogous to EU DORA’s “oversight fees.”

New Powers for Secretary of State

The government is considering granting the Secretary of State the power to issue directions to regulated entities to address cybersecurity issues. This could, for example, include directions to take actions to address critical vulnerabilities of IT systems, or to take specified actions to address incidents affecting IT systems. The Secretary of State would only be able to exercise these powers in response to threats to national security.

These “national security” directions powers will likely be more flexible than those given to regulators under the EU’s NIS2, but are similar to those introduced by Australia’s Security of Critical Infrastructure Act 2018. Notably, unlike NIS2, the proposed new enforcement powers do not include personal liability for members of management bodies.

Conclusion

Although the UK government’s reforms are still at an early stage, EU reforms provide a preview of what to expect and – for companies that are already active in the EU – provide a blueprint for compliance. Companies operating in regulated sectors should consider:

- Assessing whether they are captured by the Bill and its analogous EU reforms.
- Reviewing and stress-testing incident response plans, to ensure that:
 - They are capable of supporting the extremely quick decision-making required to meet the EU and UK’s new 24-hour incident notification windows.
 - They address how the company would respond to potentially wide-ranging directions issued to them by the Secretary of State, particularly if those directions could have significant operational impacts (*e.g.*, directions to disconnect certain systems from the internet).
- Updating cybersecurity standards and policies, particularly business continuity plans, to ensure that:
 - They reflect a level of investment and robustness that is commensurate with the UK government’s increasing expectations and tougher scrutiny of companies’ cybersecurity maturity.
 - They are aligned with, and support compliance with, UK and EU cybersecurity obligations.
- Strategically designing NIS2 compliance programs to align with the Bill, to ensure that EU compliance work already being undertaken can also support compliance with the UK reforms.